CLAIMS

1. A monolithic semiconductor integrated circuit for selectively encrypting or decrypting data transmitted between one of a plurality of devices on the circuit and an external memory, the devices each having a unique identifier comprising:
   - a cryptographic circuit arranged to encrypt or decrypt data;
   - a plurality of selectable data routes formed from a plurality of data pathways, along which data may flow between the devices and the external memory, wherein at least one data route passes through the cryptographic circuit and at least one data route does not pass through the cryptographic circuit; and
   - a control arranged to receive the identification of a selected one of the devices transferring data, and to select one of the data routes that passes through the cryptographic circuit, or one of the data routes that does not pass through the cryptographic circuit, according to the identification of the selected device.

2. A semiconductor circuit according to claim 1 wherein the control is further arranged to select a route that passes through the cryptographic circuit if the control determines that the device transferring data is secure.

3. A semiconductor circuit according to claim 1 wherein the control is further arranged to select a route that does not pass through the cryptographic circuit if the control determines that the device transferring data is insecure.

4. A semiconductor circuit according to claim 2 or 3 wherein the control is arranged to use the identification to determine that the selected device is secure or insecure.

5. A semiconductor circuit according to claim 4 wherein the control is further arranged to use the identification as an index to a look-up table containing an indication of which of the devices are secure or insecure.

6. A semiconductor circuit according to any preceding claim wherein the plurality of devices includes at least one of, a cryptographic processor, direct memory access unit, central processing unit, moving picture experts group decoder, read only memory, programmable transport interface, universal serial bus interface, or broadcast receiver.

7. A semiconductor circuit according to any preceding claim wherein the data includes video data, audio data, encryption keys, or data broadcast over air.

8. A semiconductor circuit according to any preceding claim, further arranged to transmit data from a first device to the external memory, wherein the data is selectively encrypted only if the first device is secure, and to transmit the data from the external memory to a second device, wherein the data is selectively decrypted only if the second device is secure.

9. A semiconductor circuit according to any preceding claim wherein the external memory is separated into a plurality of mutually exclusive regions, and the circuit further comprises:
   - a register for storing data for distinguishing the regions of the external memory; and
   - a filter through which the data routes connecting the devices and the external memory pass, arranged to selectively block data accesses to or from the external memory according to the identification of the device requesting the data access, and according to which region of the external memory is being accessed.

10. A semiconductor integrated circuit according to claim 9 wherein some of the regions of the external memory store privileged data, and the other regions of the external memory store unprivileged data.

11. A semiconductor integrated circuit according to claim 9 or 10 wherein the register is arranged to store the start and end memory addresses of each region of the external memory.

12. A semiconductor integrated circuit according to claim 11 wherein the filter is arranged to compare the memory address of the data being accessed with the contents of the register to determine which region of the external memory is being accessed.

13. A semiconductor integrated circuit according to claim 12 wherein the filter is arranged to selectively block data accesses requested by secure devices to unprivileged regions of data.

14. A semiconductor integrated circuit according to claim 12 wherein the filter is arranged to selectively block data accesses requested by insecure devices to privileged regions of data.

15. A television decoder comprising the semiconductor circuit according to any preceding claim.

16. A method for selectively encrypting or decrypting data transmitted between one of a plurality of devices, the devices each having a unique identifier, and an external memory, the data being transmitted along one of a plurality of selectable data routes formed from a plurality of data pathways, wherein at least one data route passes through a cryptographic circuit and at least one data route does not pass through the cryptographic circuit, comprising the steps of:
   - receiving the identification of a selected one of the devices;
   - selecting a data route that either passes through the cryptographic circuit, or one of the data routes that does not pass through the cryptographic circuit, according to the identification of the selected device.

17. The method according to claim 16 further comprising the steps of determining that the device transferring data is secure, and selecting a data route that passes through the cryptographic circuit if the device is secure.

18. The method according to claim 16 further comprising the steps of determining that the device transferring data is insecure, and selecting a data route that does not pass through the cryptographic circuit if the device is insecure.

19. The method according to claim 17 or 18 further comprising the step of using the identification to determine that the selected device is secure or insecure.

20. The method according to claim 19 further comprising the step of using the identification as an index to a look-up table containing an indication of which of the devices are secure or insecure.

21. The method according to any of claims 16 to 20 wherein the plurality of devices includes at least one of, a crypto core, direct memory access unit, central processing unit, moving picture experts group decoder, read only memory, programmable transport interface, universal serial bus interface, or broadcast receiver.

22. The method according to any of claims 16 to 21 wherein the data includes video data, audio data, encryption keys, or data broadcast over air.

23. The method according to any of claims 16 to 22 further comprising the steps of:

- transmitting data from a first device to the external memory;
- selectively encrypting the data only if the first device is secure;
- transmitting the data from the external memory to a second device; and
- selectively decrypting the data only if the second device is secure.

24. The method according to any of claims 16 to 23 wherein the external memory is separated into a plurality of mutually exclusive regions, the method further comprising the steps of:
    - determining which region of the external memory is being accessed;
    - selectively blocking the data accesses to or from the external memory according to the identification of the device requesting the data access, and according to which region of the external memory is being accessed.

25. The method according to claim 24 wherein some of the regions of the external memory store privileged data, and the other regions of the external memory store unprivileged data.

26. The method according to claim 24 or 25 wherein the step of determining which region of the external memory is being accessed comprises the step of comparing the memory address of the data being accessed with the start and end memory addresses of each region of the external memory.

27. The method according to claim 26 wherein data accesses requested by secure devices to unprivileged regions of data are selectively blocked.

28. The method according to claim 26 wherein data accesses requested by insecure devices to privileged regions of data are selectively blocked.